TLP:WHITE

網路詐騙事件通報協處之經驗與挑戰

Announcement Advisory Report (ANAR)

2018-04-07

TWCERTCC-ANAR-2018004

Summary

- 由於電子商務盛行，網路上有愈來愈多的電子商務平台成立。為達商品廣告效益，許多商品利用社群媒體(如：Facebook、Line 等)的高點閱率，進行網路行銷。近期網路上出現大量的惡意賣家，利用上述特性建置一頁式商品廣告頁面，並向社群媒體購買廣告，進行網路行銷詐騙。
- 此類一頁式網路詐騙廣告頁面通常未含惡意程式碼，亦不具資安威脅，但以強調低價、免運費、7 天試用期與貨到付款等極具誘惑之優惠宣傳字眼，吸引消費者下單購買商品，造成受騙民眾財務損失。
- 為遏止一頁式網路詐騙廣告，使用者應修改社群媒體的廣告偏好設定、檢舉或取消追蹤不法之惡意賣家經營之粉絲專頁，並安裝廣告阻擋外掛程式，以減少接收惡意廣告的機會，而社群媒體則應重視並審核廣告提供商之內容合法性。

Description

由於電子商務盛行，網路上有愈來愈多的電子商務平台成立，為達商品廣告效益，許多商品利用社群媒體(如：Facebook、Line 等)的高點閱率，進行網路行銷。近期網路上出現大量的惡意賣家，利用上述特性建置一頁式商品廣告頁面，並向社群媒體購買廣告，進行網路行銷詐騙。

這些賣家通常盜用正版商品公司的影片、圖片，建置一頁式廣告資訊(如圖 1 所示)，並透過臉書或 Line 散布，以廣告商品明顯低於市場行情價格的手法，刺激並誘導使用者點選一頁式廣告連結，再利用商品促銷活動倒數計時、免運費及貨到付款等宣傳手法，吸引消費者下單購買(如圖 2 所示)。然而，一頁式購物廣告雖常宣稱消費者可在到貨後，先拆封驗貨再行付款，然而實際上由於宅配業者與報關行在配送單上均標註「不得拆封驗貨」，導致消費者被迫於未見商品實物的情況下，必須先付款再拆封驗貨，嚴重侵害消費者權益。

圖 1. 透過臉書散布一頁式廣告連結

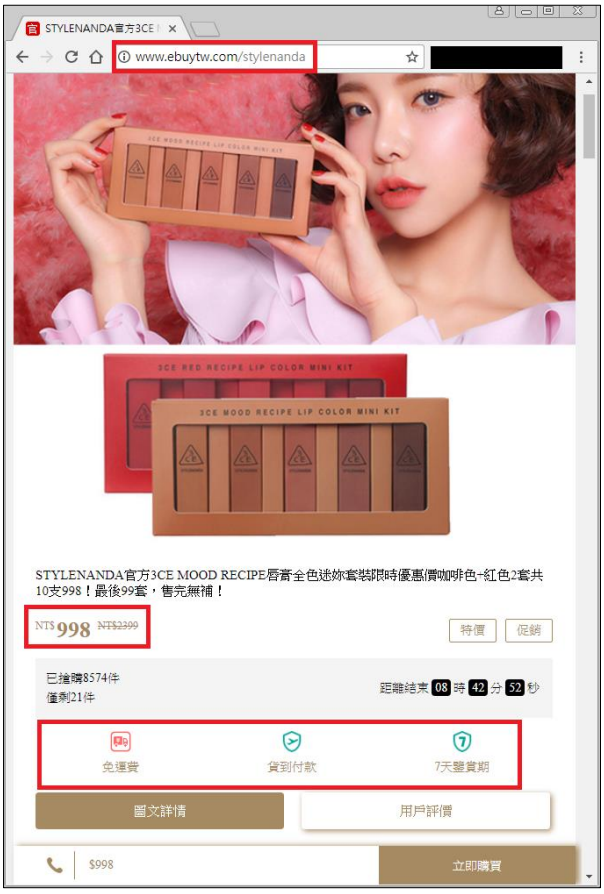

圖 2. 一頁式廣告案例

以台灣內政部警政署刑事警察局於 2018 年 3 月 27 日破獲之上海「壹加壹國際物流公司」一頁式詐騙事件為例[1]，負責人與境外詐騙集團合作，由詐騙集團擷取或變造台灣知名人物或電視台官方網站影像，結合時事、八卦等議題書面文字，在臉書粉絲專頁散布「一頁式廣告」連結，以吸引民眾上網瀏覽時點閱廣告，並誘導民眾誤信廣告內容下訂購物。該起一頁式廣告詐騙流程如圖 3 所示。

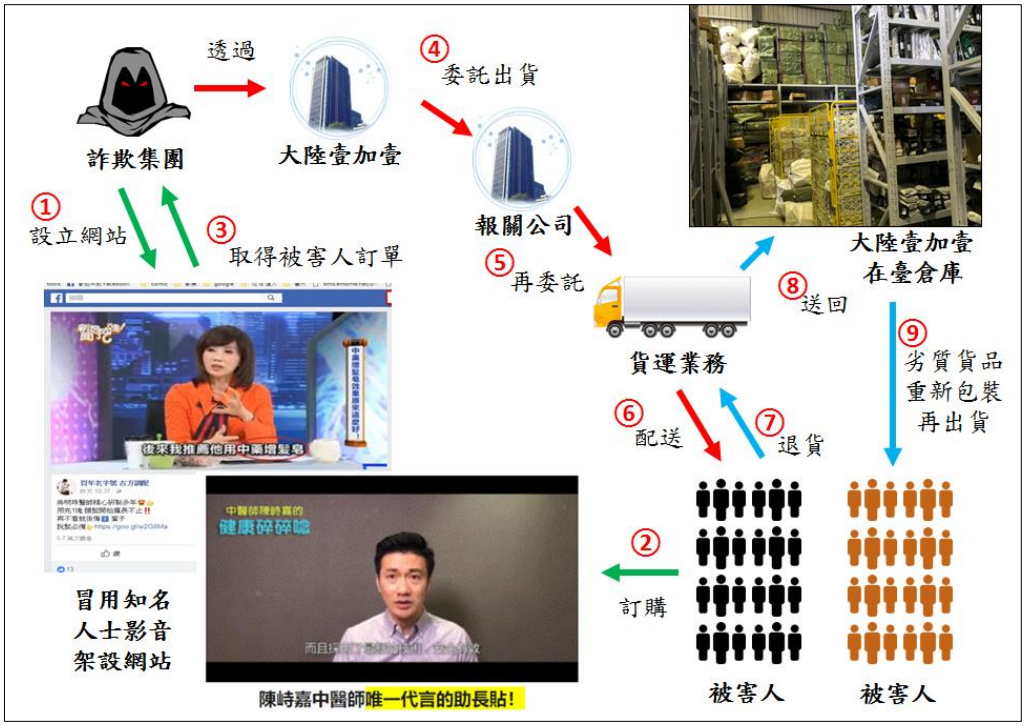

圖 3. 一頁式廣告詐騙流程

TWCERT/CC 分析刑事警察局自 2018 年 1 月 29 日起所提供之一頁式廣告網址清單共 937 筆，發現一頁式廣告以夾藏於 Facebook 連結為最大宗傳播方式(計 98 筆)，其網址多以 https://www.facebook.com/[商品相關敘述]，來誘導使用者點選並開啟廣告連結，進而選購商品。進一步清查此類一頁式廣告網址所註冊之國家，並彙整刑事局所提供之詐騙情資後，TWCERT/CC 發現詐騙集團多將一頁式廣告伺服器架設在境外，且以中國大陸居多。此外為躲避查緝，這些廣告的提供者通常在廣告釋出一週後，即再更換其他類型廣告內容，網址也隨之改變，導致追查困難度大幅提升。

雖然 TWCERT/CC 積極將可疑網址通報至所註冊之所屬國家 CERT 組織，但是針對此類通報，國際 CERT 組織通常表示：此種一頁式廣告所連結之網頁大多未含惡意程式碼，不具資安威脅，故以 CERT 權責角度，無法單以詐騙網頁為由，協助移除相關網頁或阻擋該網域；若單以詐騙網頁為由，移除合法登記註冊之廣

告專頁，恐將引起後續糾紛。有鑑於此，TWCERT/CC 目前僅以通報遭駭客利用，並以一頁式廣告方式散布的惡意廣告連結為主(如圖 4 所示)，請求國際 CERT 予以協處，以阻擋惡意連結繼續散布。

圖 4. 一頁式廣告遭 Virustotal 檢測出夾帶惡意程式碼

TWCERT/CC 分析 2018 年 3 月份由刑事局所提供之一頁式廣告連結清單，發現僅有 4.08%的廣告連結遭檢測出夾帶惡意程式碼，表示此類廣告存在資訊安全疑慮的情況仍偏低，致使社群平台、廣告業者及各國 CERT 組織直接就源頭下架或阻擋此類詐騙廣告的比例仍偏低。因此 TWCERT/CC 呼籲各國 CERT 組織、檢調單位、社群平台及廣告業者應該將此類一頁式廣告內容的合法性納入協處考量，必要時檢調單位可與 CERT 組織合作追查，以有效阻擋此類廣告的流竄，降低消費者遭到詐騙而蒙受財物損失，或是被駭客植入惡意程式的可能。

Recommendations

針對如何防範透過社群媒體所散布之一頁式廣告詐騙行為，TWCERT/CC 除呼籲社群媒體應重視並審核廣告之內容合法性以外，並彙整此類詐騙廣告特色[3]、目前本中心因應作為，及提供民眾初步防護方式如下：

一、詐騙廣告六大特色：

特徵 1：網頁上未標明公司地址及客服電話，僅留電子信箱。

特徵 2：售價下殺 1 折、3 折，明顯低於市場行情。

特徵 3：以倒數計時、存貨不多等吸引民眾，但時間、庫存永遠倒數不完。

特徵 4：免運費，且號稱有 7 天鑑賞期，並可拆箱驗貨。

特徵 5：只能使用貨到付款或信用卡付款(若消費者使用信用卡付款，將有被盜刷的風險)。

特徵 6：網頁常有簡體字或中國大陸用語(例如：支付、直郵、郵費、信息)。

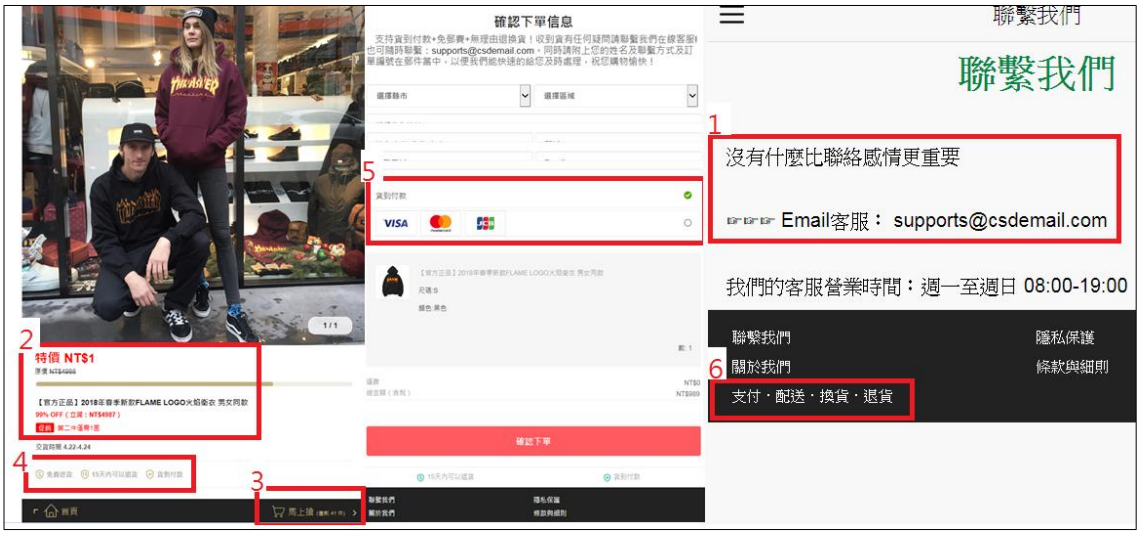

圖 5. 一頁式廣告特徵

使用者瀏覽網頁時，若發現上述特徵(如圖 5 所示)，應立即關閉所瀏覽之網頁。

二、本中心針對一頁式詐騙廣告之因應作為：

1. 密集實施主題式多元宣導

透過 TWCERT/CC 官方網站與臉書專頁及發布新聞稿，宣導民眾勿點擊一頁式廣告購物。

2. 協調國際合作防制

由於一頁式詐騙廣告網址多為國外網域，難以溯源追查，刑事警察局爰自 107 年 1 月 29 日起，按週提供「詐騙反饋平臺」詐騙網址

資料予本中心，以協助通報各國 CERT 進行分析處置。

三、本中心針對如何減少遭一頁式廣告詐騙之初步防護建議：

1. 使用者可利用第三方支付機制，確認貨品無誤再付款，並選擇評價良好、具有實體店面的賣家，以增進交易安全之保障。

2. 使用者應詳閱社群媒體所宣告之隱私權政策，修改個人之廣告偏好，並減少以社群媒體帳號登入其他服務。

3. 使用者可於瀏覽器安裝廣告阻擋外掛程式，例如 Adblock Plus[4]或 AdGuard[5]，以阻擋已知的惡意廣告連結。

4. 使用者若發現不法臉書粉絲團散布詐騙廣告，應該主動取消追蹤該粉絲團(如圖 6 所示)，或者進一步向臉書檢舉該頁面散布不實廣告(如圖 7 所示)，以減少接收惡意廣告的機會。

圖 6. 暫停追蹤可疑的臉書粉絲團

圖 7. 透過臉書封鎖及檢舉粉絲專頁

References

[1] 刑事警察局. (2018, March 29). "「詐騙爛貨復活倉儲！滿坑滿谷肚臍貼！」偵破臉書一頁式廣告販售偽劣貨詐欺案", Retrieved April 7, 2018, from the World Wide Web: https://www.cib.gov.tw/News/Detail/34194

[2] 聯合新聞網. (2018, March 28). "臉書一頁式廣告賣劣質品 爛貨全來自大陸", Retrieved April 7, 2018, from the World Wide Web: https://udn.com/news/story/7320/3056775

[3] 台北市政府警察局防制詐騙中心. (2018, January 11). "新興詐欺手法專案報告 六大特徵，破解一頁式廣告詐騙!", Retrieved April 7, 2018, from the World Wide Web: http://themes.gov.taipei/ct.asp?xItem=380501579&ctNode=45816&mp=10800d

[4] Adblock Plus. "Adblock Plus", Retrieved April 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adblock-plus/cfhdojbkjhnklbpkdaibdccddilifddb?hl=zh-TW

[5] AdGuard. "AdGuard 廣告阻擋器", Retrieved April 7, 2018, from the World Wide Web: https://chrome.google.com/webstore/detail/adguard-adblocker/bgnkhhnnamicmpeenaelnjfhikgbkllg?hl=zh-TW

聯繫資訊

台灣電腦網路危機處理暨協調中心

- 免付費專線：0800-885-066
- 資安事件通報 03-4115387 或 02-23776418
- 電子郵件：twcert@cert.org.tw
- 官方網站：https://www.twcert.org.tw/
- Facebook: http://www.facebook.com/twcertcc